

Re: Fingerprinting Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-05/0004.html>

From: Demetrio Carrión (demetrio.carrion_at_gmail.com)

Date: 05/06/05

Date: Fri, 6 May 2005 16:19:38 -0300

To: pen-test@lists.securityfocus.com

Hi,

I think of a particular case where you are able to sniff layer two traffic in the firewall segment and this firewall is an appliance-based one.

Would it possible to discover the firewall vendor by correlating the firewall MAC layer address and the OUI, then someone could narrow the firewall to a specific vendor and possible versions?

Just guessing.

Cheers,

Demetrio Carrion
IT Security Consultant

On 4/8/05, Byron L. Sonne <blsonne@rogers.com> wrote:

>
>> *We all know that, we can identify firewall using various methods and tools like "firewalk".*
>> *Is there any method or tool available which will remotely fingerprint and enumerate rule*
>> *base configured on the firewall?*
>
> *Well, more accurately put firewalk does not identify firewalls as much*
> *as it enumerates what kind of traffic will be passed as well as allowing*
> *you to figure out ACLs in use.*
>
> *Generally speaking I don't think you'll be able to come up with*
> *something along the lines of nmap that will allow you to determine what*
> *kind of firewall is in place. Certainly not reliably for all firewalls*
> *and in all situations; there's just too much variability in how rules can*
> *be configured or traffic scrubbed.*
>
> *What I do think is possible is the creation of a tool that will narrow*
> *the field down to a group of firewalls.*
>
> *However, I suppose that for peculiar situations, either from grievous*

SecurityFocus Penetration: Re: Fingerprinting Firewall

- > *design error or peculiar configurations, certain firewalls might stick*
- > *out like a sore thumb. But my suspicions are that would be rare.*
- >